Ashby & Associates

SUITE 511
1730 M STREET, N.W.
WASHINGTON, D.C. 20036

AREA CODE 202
TELEPHONE: 296-3840

STAT

Ashby & Associates - Systems Division has introduced a unique product that is designed to provide telephone security for audio countermeasures. This new product is the TSS-101. The system prevents a telephone from being compromised -- prevents telephone "bugging" from being used against you by an eavesdropper. The device is not a voice scrambler and has nothing to do with telephone "tapping." But think of telephone security this way -- the telephone may be used as a microphone and power supply by an eavesdropper when the instrument is not even in use. A telephone can be simply converted into a clandestine listening device even without access to the instrument and room conversations can be overheard without your consent or knowledge. Compromise of a telephone can be very costly and very dangerous to you.

The TSS is briefly described by the included brochure. We are writing because we think that this concept and product may be of interest to you and fill a real and practical need.

The TSS is now a commercial product for which patents are pending. The device is offered to the market at a low unit price to afford a cost effective approach to audio security and provide performance capabilities not otherwise available.

Purchased Quantity	Factory Retail Price per Unit (#US)
1 through 9	$149.95
10 " 25	136.00
26 " 50	129.95
51 " 100	124.95
101 " 250	119.95
251 and over	100.00

The TSS was conceived by our people whose experience and understanding of security has made them intimately familiar with audio countermeasures. Since the system has been evaluated by numerous industrial and government security groups and found to be effective, we feel that you should also have an opportunity to see and procure such a useful and effective protection system. We are pleased to offer references to qualified buyers.

Approved For Release 2004/03/31 : CIA-RDP80M01082A000100290006-8

SUITE 511
1730 M STREET, N.W.
WASHINGTON, D.C. 20036

AREA CODE 20
TELEPHONE: 296-

TSS-101 TELEPHONE COMPROMISE PROTECTION SYSTEM

PERFORMANCE SUMMARY

The TSS-101 is an effective telephone compromise protection system and offers the user the performance outlined in this summary.

A. Earpiece audio compromises protected against include:

1. Capacitor hook switch bypasses.

2. Rf transmitting devices using the earpiece as the microphone, concealed within the handset or instrument base, and using line rechargeable batteries for power.

3. Rf carrier current devices using the earpiece as the microphone and external telephone lines for propagation.

4. External rf flooding down telephone wires which use the mouth- and/or earpiece as the microphone, with or without an rf bypass capacitor around the hook switch.

5. External rf microwave illumination of passive devices using the mouth- or earpieces as the microphone.

6. Dynamic or magnetic miniature microphones installed directly across telephone lines and within 5 to 10 inches of the TSS-101.

7. Dynamic or magnetic miniature microphones connected to a miniature radio transmitter within 5 to 10 inches of the TSS-101 induction coil.

B. Bell circuitry compromises protected against include:

1. Coil or clapper sensors.

2. Magnetic or dynamic microphones attached to bell circuitry.

3. Audio bypasses to bell circuitry from the sidetone transformer terminals.

4. Secretarial buzzer lines with audio bypasses or magnetic/dynamic-type microphones attached.

In general, these compromise techniques all exploit a magnetic-type audio sensor or microphone. Since the noise coupling mechanism is magnetic also, mask coupling is most efficient and thus very effecti

C. Mouthpiece audio compromises protected against include:

1. Resistor hook switch bypasses where less than 5 ma dc flows from the telephone lines through the instrument and mouthpiece. This small amount of current prevents alerting of both telephone user and telephone company's central station.

2. Zener diode, SCR or transistor and resistor hook switch bypasses wherein the semiconductor acts as a switch controllable by the eavesdropper and the resistor limits current flows to a minimum to prevent detection.

3. Neon bulb bypasses are similar to C-2 but very small amounts of current flow and the miniature bulb is a gaseous high voltage switching device controlled by the eavesdropper.

4. Resistor and capacitor hook switch bypasses wherein small dc currents flow and audio is passed more freely through the compromise network to the outside lines.

5. Microwave illumination or rf flooding using the mouthpiece as the audio modulating resistance.

6. Low impedance compromises where 60 to 100 ma flow through the instrument and protection is dependent upon room conversation audio level. Limited (15 to 20%) audio is perceptable when the speaker is within two feet of the instrument and uses a loud voice.

C-6 compromises, e.g., infinity transmitter, bent hook switch, are very alerting to both the telephone user (line apears "open" or has no dial tone) and the central station (line appears "busy" no incoming calls are completed, line is unused). The percentage of occurrence in today's professional surveillance environment is very small. The user's judgment or a simple volt-ohm meter continuity test easily checks for these types of compromises.

To be effective and protect against this class of penetration attempt the coil placement must be next to the sidetone transformer at the side of the instrument for optimum coupling. Furthermore, the unit

should be turned up to a high level jamming intensity and used only as required. When this is done, it will be necessary to turn the unit OFF while using the phone, which is not necessary for A and B because a lower level of jamming is necessary to be equally effective. The TSS-101 was designed to operate manually rather than automatically to specifically allow use on an "as needed" basis. An masking system which remains needlessly on only affords the oppositi greater opportunity for penetration through signal analysis.

The mouthpiece, though not magnetic, is connected directly to the sidetone transformer which is magnetic and thus jammed by the TSS-10: In addition, the earpiece itself generates small amounts of audible noise which in most cases is propagated through the handle cavity to the rear of the mouthpiece. If the cotton is removed and a small hole drilled in the plastic cup holding the mouthpiece, this effect is enhanced. This explains why the mouthpiece is also satisfactorily prevented from being an efficient audio pickup.

The TSS-101 will have a small or no effect on the following types of audio penetrations:

D. Telephone line taps using direct hardware connections to a recorder or radio transmitter which intercepts only telephone conversations.

E. Drop-in mouthpiece radio transmitters.

F. Unauthorized recordings made at either end of a telephone conversation.

G. Capacity, electrolyte, carbon, or ceramic microphones which are not connected to sidetone transformer circuitry but only to external lines and isolated from handset audio circuitry.

H. Use of an extension telephone to overhear other's conversations.

It should be noted that the line disconnection-type security devices are not effective against A-2, 5, 6 (microphones connected line side of disconnect), 7; C-5, 6; whereas the TSS-101 is effective. Unfortunately, the disconnect types are equally ineffective against D, E, F, G (microphones connected line side of disconnect), and H as is the TSS-101. Finally, the user cannot easily verify the operation

of a disconnect device since it too can be bypassed by any means a hook switch can; a disconnect is not portable or private, i.e., a telephone company technician should install it. The only practical solution is to disrupt the instrument's ability to sense audio; the TSS-101 does this, disconnect-type devices to not.

For all cases described above, babble audio-type noise rather than white noise will increase the overall effectiveness of the unit, especially in C-6. This could be provided from tape recorders, record players, or radios and would be an advisable addition by the customer for highly secure areas. One special source could service many 101's in a single office area. An alternative is the direct hardware connection to the sidetone transformer. The noise produced with the hard wire connection is so intense within the instrument (not on outside lines) that even H is thoroughly protected against. This last alternative is mentioned discretely because of telephone company objections to tampering with equipment.

The multiline, pushbutton telephones common to many industrial and government offices inherently afford a good deal of protection from most types of compromise. The reason for this is the extreme difficulty in preselecting a specific pair of outside lines and reaching the desired target telephone. Those compromises which are still a potential threat, however, include A-2, 5, 7; C-6; D; E; F; and H. Often overlooked is the fact that many multiline instruments have one or more direct outside lines which do not rotate through the telephone's automatic switching system. These lines would, of course, be susceptible to the single line compromises. Also, extension lines within an office area provide easy line identification and activation of a target in another's office and allow a variety of compromises.

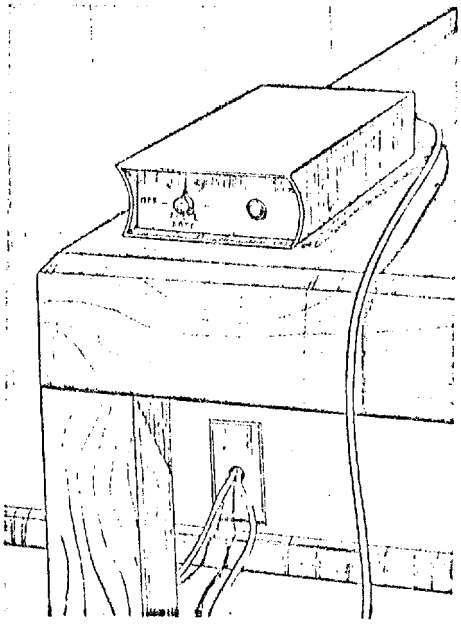
Summarizing, the TSS-101 is designed for maximum utility, ease of operation, and minimum cost with maximum effectiveness for both single and multiline telephones. It should be used as a portable system for conference rooms, motels, etc., as interim protection systems between telephone security checks, and to provide good day-to-day telephone compromise security.

TELEPHONE SECURITY SYSTEM

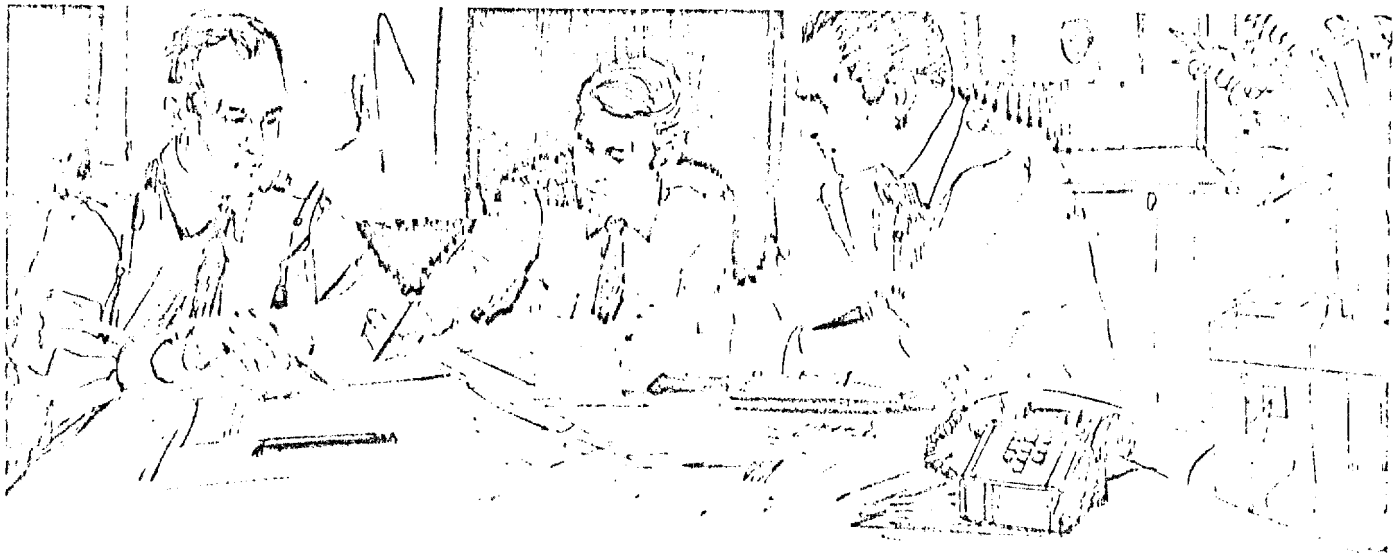
MODEL TSS 501

FOR UNAUTHORIZED LINE USE MONITORING

The infinity transmitter, a popular room bugging device is in wide spread use today by electronic eavesdroppers. It is connected anywhere along a pair of telephone wires in an office area and activated by simply calling the number from another telephone and applying an audio tone. The target telephone will never ring, but its lines are used to pass all room audio to the eavesdropper.



The TSS-501 Telephone Line Use Monitor will provide a positive indication when your line is being used for this type of electronic audio surviellance. This unit is completely automatic and self powered, requiring inexpensive batteries only once a year. The 501 is constantly on guard and its silent flashing indicator will notify you immediately when your line is being used.



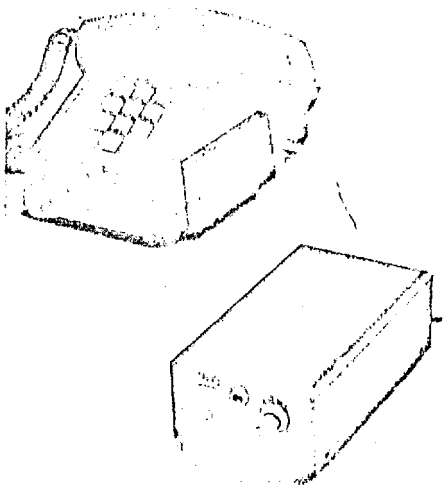
ASHBY & ASSOCIATES SYSTEMS DIVISION 1730 M STREET N. W.
WASHINGTON, D.C. 20036 (202) 659-8510

TELEPHONE SECURITY SYSTEM

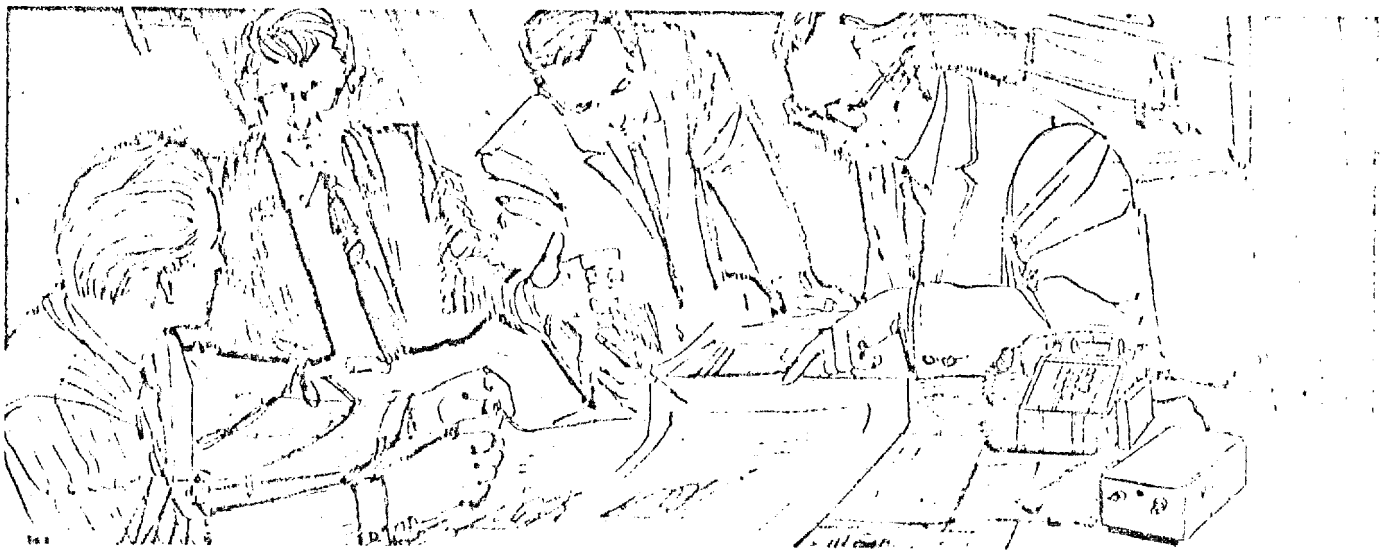
MODEL TSS 101

FOR AUDIO COMPROMISE PROTECTION

Telephones have been used for years by eavesdroppers as a convenient and reliable means to bug conference rooms, board rooms and offices simply because the unused telephone is always within reach of a sensitive business discussion. With a few simple modifications the telephone will pass room audio just as if it were left off the hook — yet remain unaffected in its normal operation. Once audio is on the lines it can go anywhere in the telephone system to be recorded by the eavesdropper.



The TSS-101-System offers proven protection from this common method of eavesdropping — the Telephone Compromise — by preventing the ever present telephone microphones from being able to receive usable room audio. This system magnetically induces an intense noise into the microphones which silently but effectively masks all room audio and makes it unusable to the eavesdropper.



ASHBY & ASSOCIATES SYSTEMS DIVISION 1730 M STREET, N. W.
WASHINGTON, D. C. 20036 PHONE: (202) 296-5840

DESCRIPTION

The TSS-101 is an effective audio countermeasures system made for use with all types of telephones both foreign and domestic. It requires no wiring or installation - - only placement of the coil module next to the telephone. The 101 is designed to prevent illegal room eavesdropping through the unused telephone instrument. It should be placed on all telephones within audible range of sensitive office discussions and is essential for the prevention of multi-line extension, outside private line and single line audio compromise penetration. The TSS-101 generates an intense magnetic audio noise which silently couples into the telephone, but not onto the outside wires. This induced noise masks the room audio received by the altered telephone and prevents it from being used by the eavesdropper. Prior to openly discussing sensitive information near an unused telephone, the TSS-101 is simply turned on and the gain adjusted. Upon meeting completion, the gain may be turned down or off to prevent needlessly alerting the would be eavesdropper. Where an unusual mask signal is required, an additional masking source may be added through the auxiliary input provided on the rear panel and mixed with the internally generated noise.

SYSTEM PERFORMANCE AND SPECIFICATIONS

The TSS-101 is the only unit available which is effective against all the following types of eavesdropping penetrations which use the telephone's audio network to pick up room conversations.

- Earpiece Compromises
- Mouthpiece Compromises
- Multi-line Extension Compromises
- Radio Transmitters
- Passive Reflectors

Size: Control Unit 3-5/8" x 2-3/8" x 7-5/8", Coil Module 1/2" x 2" x 4"
Shipping Weight: 3 lbs
Noise Masking Spectrum: 1000 Hz ± 800 Hz pseudo random without auxiliary input
Power Consumption: 110 VAC/60 Hz, 220 VAC/50-60 Hz optional, 5 watts
Color: Walnut brown standard
Controls: Unit On/Off, noise On/Off, gain and spectrum adjustment, coil output, external audio mask input.